UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/661,690	09/12/2003	**David D. Brandt**	03AB014B/ALBRP303USB	7383

7590 01/29/2010

Susan M. Donahue
Rockwell Automation, 704-P, IP Department
1201 South 2nd Street
Milwaukee, WI 53204

EXAMINER	
KIM, TAE K	

ART UNIT	PAPER NUMBER
2453	

MAIL DATE	DELIVERY MODE
01/29/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/661,690	Applicant(s) BRANDT ET AL.	
	Examiner TAE K. KIM	Art Unit 2453	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 October 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,9-22,24-29 and 32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,9-22,24-29 and 32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *01/05/10*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This is in response to the Applicant's response filed on October 9, 2009. Claims 1, 4, 10, 11, 17, 18, 20 - 22, 24 - 26, and 28 have been amended by the Applicant. Claims 1-5, 9 – 22, 24—29, and 32, where Claims 1, 17, 20, 24, 25, and 28 are in independent form, are presented for examination.

Information Disclosure Statement

The information disclosure statement (IDS) submitted on January 5, 2010 was filed after the mailing date of the RCE on April 1, 2009. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Response to Arguments

Applicant's arguments filed on October 9, 2009 have been fully considered but they are not persuasive. Applicant argued:

a) Regarding Claim 1, Salowey does not specifically disclose of "a control-specific transport mechanism for data exchange between automation assets that is adapted to include at least one security field within the extensible factory protocol."

b) Regarding Claim 1, Salowey does not specifically disclose that "the security field of the extensible factory protocol authenticates at least one of a requestor of the data or a supplier of the data."

c) Regarding Claim 10, Salowey does not specifically disclose that “the extensible factory protocol comprises a Control and Information Protocol (CIP) having a path segment that has been adapted to include a segment identifying a requestor of a connection between automation assets and employed to authenticate the requestor."

d) Regarding Claims 17, 20 and 24, neither Salowey nor Branstad discloses of "providing a security time-out within the wireless security protocol that times-out data transactions between the automation devices after a predetermined time duration until a subsequent determination of real-time data transfer requirement and network security requirements is performed.”

e) Regarding Claims 25 and 28, neither Salowey, Branstad, nor Bridges discloses of "a time component encoded in the factory protocol that defines an amount of time after which data exhcnage between control devices is timed-out until the at least one of a security or performance parameter is re-evaluated."

Examiner respectfully disagrees with applicant’s assertions.

1. With regards to a), the Applicant states that the initial authentication of a client is performed using Extensible Authentication Protocol (EAP) where the messages are exchanged between an authentication center (server) and a mobile device desiring communication with a server or other device [See Applicant’s Remarks Pg. 14, Para. 2].

The Applicant argues that communication between the mobile device and the server are not message exchanged between automation assets [See Applicant's Remarks Pg. 14, Para. 3].

The examiner points out that the pending claims must be "given the broadest reasonable interpretation consistent with the specification" [In re Prater, 162 USPQ 541 (CCPA 1969)] and "consistent with the interpretation that those skilled in the art would reach" [In re Cortright, 49 USPQ2d 1464 (Fed. Cir. 1999)]. The term "automation asset" is not specifically defined within the specification to eliminate the authentication center (server) as being an automation asset. On the contrary, the specification describes an automation asset as a computer [See Para. 0028].

The mobile device communicates with the server, which can be embedded within the access point [Col. 5, lines 13-14], to authenticate the mobile device to allow that mobile device to access the desired network coupled to the server/access point [See Fig. 1]. Therefore, communication between the mobile device and the server/access point are the exchange of messages between automation assets.

Salowey further discloses that the EAP is a control-specific transport mechanism for data exchange adapted to include at least one security field within the extensible factory protocol [Col. 6, lines 19-53; when the client communicates with a network wirelessly using the 802.1x protocol, the temporary authorization key or credential key (security field) may be transmitted within the protocol of the EAP-SIM mechanism]. Without more, there is no distinction between the pending claim and the prior art of record.

2. With regards to b), Saloway discloses that the temporary authentication key, which can be part of the short-term authentication data, is used for re-authentication the client to the server [Col. 6, lines 19-44]. Therefore, the extensible factory protocol authenticates at least one of a requestor of the data or a supplier of the data. Without more, there is no distinction between the pending claim and the prior art of record.

3. With regards to c), the arguments are directed to additional limitations that have been amended into the claim. These arguments are moot based upon new grounds of rejection provided below.

4. With regards to d), Applicant states that Branstad employs periodic heartbeat message sent from a receiver device to a sender device that contain information regarding authentication errors, CPU load information, missing packet information, and the like [See Applicant's Remarks Pg. 16, Para. 2]. Applicant, however, attempts to distinguish the "heartbeat interval" disclosed in Branstad from a "security time-out that times-out data transactions between devices after a predetermined time duration" [See Applicant's Remarks Pg. 16, Para. 2].

Branstad discloses that the “heartbeat interval” is timeout interval during which an ACSA participant should expect to receive a control message from the remote party [Col. 6, lines 5-11]. Branstad further discloses that the sender re-determines the authentication gear based on local and remote information including a notification from the receiver [Fig. 5; Col. 7, 38-54]. Furthermore, when a gear change is determined to be necessary, the sender attempts to synchronize with the receiver using a switch gear message and if the receiver does not return a gear switch acknowledgement message

before the expiration of the heartbeat interval, the sender switches back to the base gear (the most secure gear) [Fig. 7A and 7B; Col. 8, lines 23-67]. Therefore, the Branstad system uses the heartbeat interval to timeout non-base gear data transactions when the heartbeat interval lapses without a gear switch acknowledgement message and non-base gear data transactions can resume when a subsequent determination of the authentication gear is made by the sender. Without more, there is no distinction between the pending claim and the prior art of record.

5. With regards to d), the Examiner points to section 5 above describing how Branstad disclosed the time-out interval.

Claim Rejections - 35 USC § 102

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 1 – 5, 9 – 16, and 32 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 7,536,548, invented by Brian Alan Batke, et al. (hereinafter "Batke").

The applied reference has a common assignee with the instant application. Based upon the earlier effective U.S. filing date of the reference, it constitutes prior art under 35 U.S.C. 102(e). This rejection under 35 U.S.C. 102(e) might be overcome either by a showing under 37 CFR 1.132 that any invention disclosed but not claimed in the reference was derived from the inventor of this application and is thus not the invention “by another,” or by an appropriate showing under 37 CFR 1.131.

6. Regarding Claim 1, Batke discloses of an automation security system [Fig. 1 and 2], comprising:

an automation asset operatively coupled to a network communication channel [Fig. 1, Col. 4, lines 4-22], an automation asset comprises at least an automation control device [Fig. 1]and implements the following:

an extensible factory protocol to transport data between the automation asset and a remote automation asset on a remote network communication channel [Fig. 1, Col. 4, lines 4-22], the extensible factory protocol is a control-specific transport mechanism for data exchange between automation assets that is adapted to include at least one security field within the extensible factory protocol to exchange data with the remote automation asset [Col. 4, lines 23-44], the security field of the extensible factory protocol authenticates at least one of a requestor of the data or a supplier of the data [Fig. 3; Col. 2, lines 35-49; Col. 6; lines 44-62].

7. Regarding Claim 2, Batke discloses all the limitations of Claim 1 above. Batke further discloses that the security field further comprises path information to identify a requester or supplier of a connection [Col. 2, lines 35-49].

8. Regarding Claim 3, Batke discloses all the limitations of Claim 2 above. Batke further discloses that the path information facilitates non-connected data access by sending out an open-ended message [Fig. 12].

9. Regarding Claim 4, Batke discloses all the limitations of Claim 1 above. Batke further discloses that the automation asset further comprises at least one of a controller, a communications module, a computer, a sensor actuator, a network sensor, an I/O

device, Human Machine Interface (HMI), an I/O module, or a network device [Fig. 1].

10. Regarding Claim 5, Batke discloses all the limitations of Claim 1 above. Batke further discloses that the network communications channel is established across at least one of: a control network, factory network, information network, private network, instrumentation network, a wireless network, or a public network [Fig. 1, item 30].

11. Regarding Claim 9, Batke discloses all the limitations of Claim 1 above. Batke further discloses that the extensible factory protocol includes at least one of: a time component to mitigate replay attacks, a message integrity component, a digital signature, a sequence field to mitigate replaying an old packet, a pseudo random sequence, an encryption field, or a dynamic security adjustment field [Fig. 2 and 3].

12. Regarding Claim 10, Batke discloses all the limitations of Claim 1 above. Batke further discloses that the extensible factory protocol comprises a Control and Information Protocol (CIP) [Col. 2, lines 50-67] having a path segment that has been adapted to include a segment identifying a requestor of a connection between automation assets and employed to authenticate the requestor [Fig. 3; Col. 2, lines 35-49; Col. 6; lines 44-62].

13. Regarding Claim 11, Batke discloses all the limitations of Claim 1 above. Batke further discloses that the control-specific transport mechanism is further adapted to at least one of: provide source validation for identification, perform message digest checking for integrity checking, perform check sum tests, provide integrity mechanisms, provide encryption mechanisms, or provide refresh security protocols [Col. 6, lines 14-34].

14. Regarding Claim 12, Batke discloses all the limitations of Claim 1 above. Batke further discloses that the extensible factory protocol facilitates at least one of an identification, an authentication, an authorization, or a ciphersuite negotiation to establish network trusts [Fig. 3].

15. Regarding Claim 13, Batke discloses all the limitations of Claim 1 above. Batke further discloses that the extensible factory protocol is associated with a protocol supporting at least one of: a Temporal Key Interchange Protocol (TKIP) or a wireless protocol [Col. 5, lines 4-12].

16. Regarding Claim 14, Batke discloses all the limitations of Claim 1 above. Batke further discloses that the extensible factory protocol employing at least one of: an Elliptical function, an Aziz/Diffie Protocol, a Kerberos protocol, a Beller-Yacobi Protocol, an Extensible authentication protocol (EAP), an MSR+DH protocol, a Future Public Land Mobile Telecommunication Systems Wireless Protocols (FPLMTS), a Beller-Chang-Yacobi Protocol, a Diffie-Hellman Key Exchange, a Parks Protocol, an ASPECT Protocol, a TMN Protocol, RADIUS, Groupe Special Mobile (GSM) protocol, or a Cellular Digital Packet Data (CDPD) protocol [Col. 5, lines 29-49].

17. Regarding Claim 15, Batke discloses all the limitations of Claim 1 above. Batke further discloses that the network communications channel employing at least one of: a Control and Information Protocol (CIP) network, a DeviceNet network, a ControlNet network, an Ethemet network, DH/DH+ network, a Remote I/O network, a Fieldbus network, or a Profibus network [Col. 2, line 62 – Col. 3, line 4].

18. Regarding Claim 16, Batke discloses all the limitations of Claim 1 above. Batke

further discloses of a security field to limit access based upon line of sight parameters [Col. 5, lines 4-15].

19. Regarding Claim 32, Batke discloses all the limitations of Claim 1 above. Batke further discloses that the extensible factory protocol maintains backward compatibility with an automation asset incapable of implementing the security field [Fig. 12].

Claims 1 – 5, 9 – 16, and 32 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 7,370,350, invented by Joseph Salowey (hereinafter "Salowey").

20. Regarding Claim 1, Salowey discloses an automation security system [Fig. 1], comprising:

an automation asset operatively coupled to a network communication channel, an automation asset comprises at least an automation control device [Fig. 1; client device coupled to and access point and the assets within the secure network] and implements the following:

an extensible factory protocol to transport data between the automation asset and a remote automation asset on a remote network communication channel [Col. 4, Lines 31-41; initial EAP-SIM authentication], the extensible factory protocol is a control-specific transport mechanism for data exchange between automation assets that is adapted to include at least one security field within the extensible factory protocol to exchange data with the remote automation asset [Fig. 2B; authentication data comprises temporary authentication key and is encrypted using initial authentication session key], the security field of the extensible factory protocol authenticates at least

one of a requestor of the data or a supplier of the data [Fig. 2B; policy data is user identity value; Col. 6, lines 19-44].

21. Regarding Claim 2, Salowey discloses all the limitations of Claim 1 above. Salowey further discloses that the security field further comprises path information to identify a requester or supplier of a connection [Fig. 2B; policy data is user identity value].

22. Regarding Claim 3, Salowey discloses all the limitations of Claim 2 above. Salowey further discloses that the path information facilitates non-connected data access by sending out an open-ended message [Fig. 2B, items 216, 218, 220].

23. Regarding Claim 4, Salowey discloses all the limitations of Claim 1 above. Salowey further discloses that the automation asset further comprises of a controller, a communications module, a computer, a sensor actuator, a network sensor, an I/O device, a Human Machine Interface (HMI), an I/O module, or a network device [Fig. 1; computer].

24. Regarding Claim 5, Salowey discloses all the limitations of Claim 1 above. Salowey further discloses that the network communications channel is established across at least one of: a control network, factory network, information network, private network, instrumentation network, a wireless network, or a public network [Fig. 1; Col. 4, Lines 55-59; wireless network].

25. Regarding Claim 9, Salowey discloses all the limitations of Claim 1 above. Salowey further discloses that the extensible factory protocol includes at least one of: a time component to mitigate replay attacks, a message integrity component, a digital

signature, a sequence field to mitigate replaying an old packet, a pseudo random sequence, an encryption field, or a dynamic security adjustment field [Fig. 2B; credential is encrypted using private key of the server].

26. Regarding Claim 11, Salowey discloses all the limitations of Claim 1 above. Salowey further discloses that the control-specific transport mechanism is further adapted to at least one of: provide source validation for identification, perform message digest checking for integrity checking, perform check sum tests, provide integrity mechanisms, provide encryption mechanisms, or provide refresh security protocols [Fig. 2B; reauthentication of first computing device using challenge-response mechanism].

27. Regarding Claim 12, Salowey discloses all the limitations of Claim 1 above. Salowey further discloses that the extensible factory protocol facilitates at least one of an identification, an authentication, an authorization, or a ciphersuite negotiation to establish network trusts [Fig. 2B; policy data is user identify value].

28. Regarding Claim 13, Salowey discloses all the limitations of Claim 1 above. Salowey further discloses that the extensible factory protocol is associated with a protocol supporting at least one of: a Temporal Key Interchange Protocol (TKIP) or a wireless protocol [Fig. 1; Col. 4, Lines 55-59; wireless network].

29. Regarding Claim 14, Salowey discloses all the limitations of Claim 1 above. Salowey further discloses that the extensible factory protocol employing at least one of: an Elliptical function, an Aziz/Diffie Protocol, a Kerberos protocol, a Beller-Yacobi Protocol, an Extensible authentication protocol (EAP), an MSR+DH protocol, a Future Public Land Mobile Telecommunication Systems Wireless Protocols (FPLMTS), a

Beller-Chang- Yacobi Protocol, a Diffie-Hellman Key Exchange, a Parks Protocol, an ASPECT Protocol, a TMN Protocol, RADIUS, Groupe Special Mobile (GSM) protocol~ [[and]] or a Cellular Digital Packet Data (CDPD) protocol [Fig. 2B; EAP-SIM authenticaiton].

30. Regarding Claim 15, Salowey discloses all the limitations of Claim 1 above. Salowey further discloses that the network communications channel employing at least one of- a Control and Information Protocol (CIP) network, a DeviceNet network, a ControlNet network, an Ethemet network, DH/DH+ network, a Remote I/O network, a Fieldbus network, or a Profibus network [Fig. 1; network access point using wireless protocol (Remote I/O network)].

31. Regarding Claim 16, Salowey discloses all the limitations of Claim 1 above. Salowey further discloses of a security field to limit access based upon line of sight parameters [Fig. 1; network access point using wireless protocol].

32. Regarding Claim 32, Salowey discloses all the limitations of Claim 1 above. Salowey further discloses that the extensible factory protocol maintains backward compatibility with an automation asset incapable of implementing the security field [Fig. 2B; reauthentication of first computing device to second computing device using challenge-response mechanism].

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Salowey, in view of U.S. Appl. 2002/0120728, filed by Jason Braatz, et al. (hereinafter "Braatz").

33. Regarding Claim 10, Salowey discloses all the limitations of Claim 1 above. Salowey, however, does not specifically disclose that the extensible factory protocolcomprises a Control and Information Protocol (CIP)having a path segment that has been adapted to include a segment identifying a requestor of a connection between automation assets and employed to authenticate the requestor.

Braatz discloses a network and system that provides control, monitoring, security, and convenience of operation of one or more interconnected devices [Para. 0013]. The interconnected devices use Object Control and Information Protocol that comprises of a header with fields that identify the destination and source devices of the communication [Fig. 6]. Braatz further discloses that this protocol can be transmitted over any medium, including TCP/IP and WAP.

It would have been obvious to one skilled in the art to incorporate the teaching of Braatz in the Salowey system since the Salowey system utilizes TCP/IP to communicate with the industry control system.

The motivation to do so is to make better use of the feature-rich devices and information content available today and to allow a more integrated solution to management of a number of devices, as well as the ability to monitor and communicate with the devices at a reasonable cost [Para. 0012].

Claims 17 - 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Salowey, in view of U.S. Patent 6,842,860, invented by Dennis K. Branstad et al. (hereinafter "Branstad").

34. Regarding Claims 17, 20, 21, and 24, all the limitations of Claim 1 as stated above. Salowey further discloses the user of a web browser and a web server for the authentication process [Col. 4, Lines 55-66]. Therefore, Salowey can use TCP/IP to communicate with the web server.

Salowey, however, does not specifically disclose of determining real-time data transfer requirements for automation devices in an industrial automation system; dynamically selecting a first encryption mechanism for the wireless security protocol during data transfers having a performance requirement exceeding a predetermined level, and selecting a second encryption mechanism for the wireless security protocol during data transfers having a performance requirement below the predetermined level, the second encryption mechanism providing a higher degree of encryption than the first encryption mechanism; and providing a security time-out within the wireless security protocol that times-out data transactions between the automation devices after a predetermined time duration until a subsequent determination of real-time data transfer requirements and network security requirements is performed.

Branstad discloses the use of various levels of security authentication mechanisms depending on various system conditions regarding security authentication speeds with message authentication codes (used to authenticate sender or requestor of data) standard to security protocol IPSec (part of the Internet Protocol suite TCP/IP)

[Fig. 3; Col. 3, Lines 43-49, 54-56; Col. 4, Lines 2-7, 53-61]. Branstad also discloses that the authentication system is designed to adaptively adjust its authentication strength and speed to meet current needs based on consideration such as security policy (desired security levels), observed authentication error rates, alarms from host or network defenses, and processor loading (real-time communication performance) [Col. 4, lines 2-7]. Branstad further discloses that the authentication gear is switch to a less secure gear if the sender or receiver is too heavily loaded (performance level below a predetermined level) for the performance needs of the system and to a more secure gear if both the sender and receiver are lightly loaded (performance exceeding a predetermined threshold) [Fig. 6; Col. 8, lines 4-14].

Additionally, Branstad discloses that the “heartbeat interval” is timeout interval during which an ACSA participant should expect to receive a control message from the remote party [Col. 6, lines 5-11]. Branstad further discloses that the sender re-determines the authentication gear based on local and remote information including a notification from the receiver [Fig. 5; Col. 7, 38-54]. Furthermore, when a gear change is determined to be necessary, the sender attempts to synchronize with the receiver using a switch gear message and if the receiver does not return a gear switch acknowledgement message before the expiration of the heartbeat interval, the sender switches back to the base gear (the most secure gear) [Fig. 7A and 7B; Col. 8, lines 23-67]. Therefore, the Branstad system uses the heartbeat interval to timeout non-base gear data transactions when the heartbeat interval lapses without a gear switch

acknowledgement message and non-base gear data transactions can resume when a subsequent determination of the authentication gear is made by the sender.

It would have been obvious to one skilled in the art to incorporate the teaching of Branstad in the Salowey system since the Salowey system utilizes TCP/IP to communicate with the industry control system. TCP/IP allows the use of the IPSec security protocol to secure communications within a communication network.

The motivation to combine, as disclosed in Branstad, is that the levels of security at one level may make network connections too slow to process real-time high-speed video [Col. 1, Lines 26-34] and that selectively authenticating data, as described above, is a method to remedy that issue.

35. Regarding Claim 22, Salowey, in view of Branstad, discloses all the limitations of Claim 20 above. Branstad further discloses that the lightweight security protocol includes at least one of an encryption field [Col. 5, lines 17-22; high-speed, lower-strength mechanisms include partial message authentication codes (PMAC), which is a hash-based encryption system].

36. Regarding Claim 23, Salowey, in view of Branstad, discloses all the limitations of Claim 20 above. Swales further discloses of a component to identify a requestor of data [Col. 4, lines 37-43; user list and associated password used to determine access to system].

37. Regarding Claims 18 and 19, Salowey, in view of Branstad, discloses all the limitations of Claim 17 above. However, Salowey nor Branstad specifically discloses

that the factory protocol is associated with a protocol supporting at least one of a Temporal Key Interchange Protocol (TKIP).

It is commonly known to one of ordinary skill in the art that various wireless, including those using line of sight parameters, and communication protocols can be used within an automated factory network, such as CIP, TKIP, EAP, Aziz/Diffie Protocol, Kerberos protocol, Beller-Yacobi Protocol, MSR+DH protocol, FPLMTS, Beller-Chang-Yacobi Protocol, Diffie-Hellman Key Exchange, Parks Protocol, ASPECT Protocol, TMN Protocol, RADIUS, GSM protocol, and CDPD protocol. It would have been obvious to one skilled in the art at the time of the invention that a method of providing network security, such as the one described in Salowey or Branstad, would be adaptable and implemented on multiple network protocols that existed at that time. It would have also been obvious that a method of providing network security can "tunnel" through multiple types of networks that use such network protocol, such as the ones described above. Furthermore, the use of the various combinations of the aforementioned components for any communication and security protocol ensures proper transmission and authorized access of information across a network. The broad compatibility within networks and protocols available follows within the concept of allowing various components, which are more than likely to be manufactured by different vendors, to communicate seamlessly. Allowing access to the factory network wirelessly, virtually, or remotely improves the accessibility of the network and communications between an authorized user and component or between components.

Claims 25 - 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Salowey, in view of Branstad, and further in view of "AI Techniques Applied to High Performance Computing Intrusion Detection" by Susan M. Bridges et al. (hereinafter referenced as "Bridges").

38. Regarding Claims 25—29, Salowey discloses all the limitations of Claim 1 as stated above. Salowey further discloses the user of a web browser and a web server for the authentication process [Col. 4, Lines 55-66]. Therefore, Salowey can use TCP/IP to communicate with the web server.

Salowey, however, does not specifically disclose that the factory protocol utilizes at least one security field to authenticate at least one of a requestor of the data and a supplier of the data, the security field provides at least one of a security parameter or a performance parameter, or that the factory protocol is dynamically changed or adjusted based upon considerations of desired security levels and real time communications performance and employs a first and second encryption mechanism in which the second encryption mechanism provides a higher degree of encryption than the first encryption mechanism, or a time component encoded in the factory protocol that defines an amount of time after which data exchange between control devices is time—out until the at least one of a security or performance parameter is re-evaluated. Nor does Swales specifically disclose the utilization of an intrusion detection component or methodology.

Branstad discloses the use of various levels of security authentication mechanisms depending on various system conditions regarding security authentication

speeds with message authentication codes (used to authenticate sender or requestor of data) standard to security protocol IPSec (part of the Internet Protocol suite TCP/IP) [Fig. 3; Col. 3, Lines 43-49, 54-56; Col. 4, Lines 2-7, 53-61]. Branstad also discloses that the authentication system is designed to adaptively adjust its authentication strength and speed to meet current needs based on consideration such as security policy (desired security levels), observed authentication error rates, alarms from host or network defenses, and processor loading (real-time communication performance) [Col. 4, lines 2-7]. Branstad further discloses that the authentication gear is switch to a less secure gear if the sender or receiver is too heavily loaded (performance level below a predetermined level) for the performance needs of the system and to a more secure gear if both the sender and receiver are lightly loaded (performance exceeding a predetermined threshold) [Fig. 6; Col. 8, lines 4-14].

Additionally, Branstad discloses that the “heartbeat interval” is timeout interval during which an ACSA participant should expect to receive a control message from the remote party [Col. 6, lines 5-11]. Branstad further discloses that the sender re-determines the authentication gear based on local and remote information including a notification from the receiver [Fig. 5; Col. 7, 38-54]. Furthermore, when a gear change is determined to be necessary, the sender attempts to synchronize with the receiver using a switch gear message and if the receiver does not return a gear switch acknowledgement message before the expiration of the heartbeat interval, the sender switches back to the base gear (the most secure gear) [Fig. 7A and 7B; Col. 8, lines 23-67]. Therefore, the Branstad system uses the heartbeat interval to timeout non-base

gear data transactions when the heartbeat interval lapses without a gear switch acknowledgement message and non-base gear data transactions can resume when a subsequent determination of the authentication gear is made by the sender.

It would have been obvious to one skilled in the art to incorporate the teaching of Branstad in the Swales system since the Salowey system utilizes TCP/IP to communicate with the industry control system. TCP/IP allows the use of the IPSec security protocol to secure communications within a communication network.
The motivation to combine, as disclosed in Branstad, is that the levels of security at one level may make network connections too slow to process real-time high-speed video [Col. 1, Lines 26-34] and that selectively authenticating data, as described above, is a method to remedy that issue.

Branstad further discloses that the authentication system is designed to adaptively adjust its authentication strength and speed based on alarms from hosts [Col. 4, lines 2-7]. Branstad, however, does not specifically disclose the utilization of an intrusion detection component or methodology to trigger those alarms.

Bridges discloses a system and method of using artificial intelligence within a high performance computer environment detect intrusions in the network. Specifically, Bridges discloses its use within a cluster computing architecture using both TCP/IP and Giganet networking protocols [pg. 1, paragraph 3]. The system combines both anomaly and misuse detection mechanisms and uses both network traffic and system audit date as inputs, meaning the intrusion detection is both host and network-based [pg. 1, paragraph 1]. Fuzzy logic is used with association rules and frequent episodes to "learn"

normal patters of the system behavior. If certain events leave a set of patterns that are below a specified threshold, the system issues an alarm. The system can also implement rules that match patters of known attacks or patterns that are commonly associated with suspicious behavior to identify attacks [pg. 2, paragraph 5]. The system also uses a Decision Module determine the security actions once an attack is detected [pg. 9, paragraph 1]

It would have been obvious to one skilled in the art at the time of the invention to combine the teachings of Bridges with the automation security system in Salowey by including the intrusion detection module in the web server that provides the website that accesses the automation system.

The motivation to do so is so the automation security system will monitor for intrusions and unauthorized access is necessary due to the possibility of address spoofs or tunneling into the network. The Bridges system particularly functions well in an automated system where performance degradation is generally not acceptable. Furthermore, the ability of the Bridges system to use multiple communication protocols that are also usable in an automated security system makes the Bridges system very desirable as an intrusion detection system.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Contacts

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tae K. Kim, whose telephone number is (571) 270-1979. The examiner can normally be reached on Monday - Friday (8:00 AM - 5:00 PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Thomas, can be reached on (571) 272-6776. The fax phone number for submitting all Official communications is (703) 872-9306. The fax phone number for submitting informal communications such as drafts, proposed amendments, etc., may be faxed directly to the examiner at (571) 270-2979.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at (866) 217-9197 (toll-free).

/Tae K. Kim/

Tae K. Kim
Examiner, Art Unit 2453

January 25, 2010

/Liangche A. Wang/
Primary Examiner, Art Unit 2453